RAGÁLYI KÖZÖS ÖNKORMÁNYZATI HIVATAL

CSELEKVÉSI TERV

az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény, valamint a 41/2015. (VII. 15.) BM rendelet által előírt biztonsági osztály és szint elérésére

Jóváhagyom!

Zelenka Andrea sk.

jegyző

Kelt.: 2021. január 18.

TARTALOMJEGYZÉK

BEVEZETÉS

Jelen dokumentum célja, hogy a Ragályi Közös Önkormányzati Hivatal (továbbiakban: Hivatal) számára rögzítse azokat az intézkedéseket, amelyek az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben (továbbiakban: Ibtv.) valamint a 41/2015. (VII. 15.) BM rendeletben és a MÁK Kiadás dátuma: 2018.06.18. verziószám: 2.0 „Tájékoztatás az önkormányzati ASP rendszerekhez csatlakozáshoz megvalósítandó informatikai biztonsági követelményekről" előírt biztonsági szint eléréséhez szükségesek.

Területi hatály:

Ragályi Közös Önkormányzati Hivatal (3724 Ragály, Rákóczi Ferenc út 16.)

Aggtelek Község Önkormányzata (3759 Aggtelek, Kossuth Lajos út 8.)

Alsószuha Község Önkormányzata (3726 Alsószuha, Dózsa György út 3.)

Imola Község Önkormányzata (3725 Imola, Kossuth út 35.)

Jósvafő Község Önkormányzata (3758 Jósvafő, Petőfi Sándor utca 42.)

Kánó Község Önkormányzata (3735 Kánó, Széchenyi utca 7.)

Ragály Község Önkormányzata (3724 Ragály, Rákóczi Ferenc út 16.)

Szuhafő Község Önkormányzata (3726 Szuhafő, Kossuth Lajos út 5.)

Trizs Község Önkormányzata (3724 Trizs, Petőfi Sándor út 19.)

Zubogy Község Önkormányzata (3723 Zubogy, Szabadság út 51.)

Az Ibtv. 7. §-ának (1) bekezdése alapján a szervezet elektronikus információs rendszereit a kockázatarányos védelem megvalósítása érdekében biztonsági osztályba kell sorolni.

Az Ibtv. 9. §-ának (1) bekezdése alapján a szervezet védelmi felkészültsége alapján a szervezetet biztonsági szintbe kell sorolni.

I. INFORMATIKAI HÁTTÉR

Az információbiztonság átvilágítás a Hivatalra terjed ki, melyek a fent említett településeken helyezkednek el. Az Internet kapcsolatot a Parisat Távközlési és Szolgáltató Kft. szolgáltató nyújtja, mely modem készüléken keresztül csatlakozik a belső hálózatokhoz. A Hivatal összesen 13 munkaállomást működtet, melyek helyi hálózati adatkapcsolókon, útválasztókon keresztül vannak összekötve. A számítógépek Windows 10 operációs rendszerrel vannak felszerelve. A hivatal törekszik a homogén környezet kialakítására. A munkaállomásokon Windows Defender, AVG Antivirus Free típusú vírusírtó és elemző programot használ. A használt perifériku eszközök, mint nyomtatók illetve szkennerek a belső hálózaton illetve lokálisan is használhatók. A Hivatal bejárása során feltárt hiányosságokra és gyengeségekre vonatkozó információkat, javaslatokat

(melyek szorosan nem tartoznak az idevonatkozó rendelet szempontrendszerébe) személyesen, szóban hívtuk fel a figyelmet.

II. INFORMÁCIÓS RENDSZEREK OSZTÁLYAINAK MEGÁLLAPÍTÁSA

A Hivatal az információs rendszereit három kategóriába sorolja:

II.1. Infrastrukturális információbiztonsági rendszer

Ebbe a kategóriába a következő rendszer elemeket sorolja:

- Telephelyek (minden olyan helyszín telephelynek minősül, ahol érzékeny/bizalmas adat bevitel, tárolás illetve feldolgozás van)
- Munkaállomások, terminálok, mobil eszközök (számítógép, notebook)
- Szerverek
- Hálózati elemek (adatkapcsoló, tűzfal, útválasztó)
- Perifériák (hálózati nyomtatók, multifunkciós eszközök, személyi nyomtatók, fax, szkenner)

II.2. Alkalmazás szintű telepített információbiztonsági rendszer

Ebbe a kategóriába tartoznak a Hivatal által telepített helyi infrastruktúráról használt informatikai rendszerek pl. Vizual Regiszter, stb.

II.3. Alkalmazás szintű online információbiztonsági rendszer

Ebbe a kategóriába tartoznak a Hivatal által használt online informatikai rendszerek, melyek üzemeltetése központilag irányított, ilyenek pl. E-adat, Takarnet, ASP, ... stb.

A Hivatalban alkalmazott rendszerek (a 41/2015.(VII.15.) BM rendelet és a NEIH által készített OVI tábla (ver.4.60) alapján) **legmagasabb elvárt biztonsági osztálya 1-es ill. 2-es, szintű továbbá a tervezett ASP rendszerek** (MÁK Kiadás dátuma: 2018.06.18. verziószám: 2.0 „Tájékoztatás az önkormányzati ASP rendszerekhez csatlakozáshoz megvalósítandó informatikai biztonsági követelményekről előírt biztonsági szint) elvárt osztálya **3. illetve 4-es szintet** határoz meg. **A jelenlegi állapot, kivétel nélkül „0" besorolású.** A Hivatal a rendszerek teljes, részletes besorolását az IBSZ –ban rögzítette.

III. A HIVATAL ELVÁRT BIZTONSÁGI SZINTJÉNEK MEGÁLLAPÍTÁSA

A fentieknek megfelelően a Hivatal elvégezte az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben, valamint a 41/2015. (VII. 15.) BM rendeletben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, Hivatal biztonsági szintbe sorolását. Mindezt a NEIH által készített SZVI tábla (ver:2.00) alapján. Ennek eredményeképpen megállapítható, hogy **a Hivatal elvárt biztonsági szintje 2-es**.

IV. A MEGLÉVŐ VÉDELMI INTÉZKEDÉSEK VIZSGÁLATA

Megtörtént a Hivatal információbiztonsági helyzetfelmérése, melynek során a meglévő védelmi intézkedések átvilágítására került sor.

V. CSELEKVÉSI TERVEK AZ ELVÁRT BIZTONSÁGI OSZTÁLY ELÉRÉSÉRE

Az Ibtv. 10. § (2) bekezdése alapján a szervezetnek a szervezet biztonsági szintjének megállapítása után 90 napon belül cselekvési tervet kell készítenie az elvárt biztonsági szint, azaz a számára előírt adminisztratív és fizikai védelmi intézkedések megvalósítására. Az 1-es biztonsági szint elérésére 1 év, utána szintenként 2 év áll a rendelkezésre a következő biztonsági szint eléréséhez.

V.1. Kockázatelemzés összegzése

Jelmagyarázat:
Értékelés: I - Igen megfelelt, N - Nem felelt meg, NA - Nem alkalmazható

Alpont	NEIH sorszám	Intézkedés típusa	Értékelés				Megjegyzés
3.1.1. SZERVEZETI SZINTŰ ALAPFELADATOK	3.1.1.1.	Informatikai biztonsági szabályzat	I	I			A szervezet rendelkezik informatikai biztonsági szabályzattal, de az elvárás pontjai közül nem mindegyik teljesül.
3.1.1. SZERVEZETI SZINTŰ ALAPFELADATOK	3.1.1.2.	Az elektronikus információs rendszerek biztonságáért felelős személy	I	I			A szervezet vezetője ki nevezett ill. kijelölt az elektronikus információs rendszer biztonságáért felelős személyt. Lejelentése folyamatban van.
3.1.1. SZERVEZETI SZINTŰ ALAPFELADATOK	3.1.1.3.	Az intézkedési terv és mérföldkövei	I	I			A szervezet készített megvalósítási tanulmányt.
3.1.1. SZERVEZETI SZINTŰ ALAPFELADATOK	3.1.1.4.	Az elektronikus információs rendszerek nyilvántartása	I	I	I	I	A szervezet vezet nyilvántartást az információs rendszereiről, mely magába foglalja a telepített illetve online programokat és azok adatait.
3.1.1. SZERVEZETI SZINTŰ ALAPFELADATOK	3.1.1.5.	Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárás	I	I			A szervezetnek van érvényes Az elektronikus információbiztonsággal kapcsolatos engedélyezési eljárása.
3.1.2. KOCKÁZATELEMZÉS	3.1.2.1.	Kockázatelemzési eljárásrend	N	N			A szervezetnek nincs érvényes kockázatelemzési eljárásrendje.
3.1.2. KOCKÁZATELEMZÉS	3.1.2.2.	Biztonsági osztályba sorolás	I	I			A szervezet rendelkezik informatikai biztonsági szabályzattal így az információs rendszerek biztonsági osztályba sorolása és annak eredményei rögzítve vannak.
3.1.2. KOCKÁZATELEMZÉS	3.1.2.3.	Kockázatelemzés	I	I			A szervezet informatikai biztonsági szabályzata rögzíti a kockázatelemzéseket és annak eredményeit.
3.1.3. RENDSZER ÉS SZOLGÁLTATÁS BESZERZÉS	3.1.3.6..	Külső elektronikus információs rendszerek szolgáltatásai	I	I			Információbiztonsági követelmények hiányában a szervezet nem ellenőrzi az igénybe vett külső információs rendszereket.
3.1.4. Üzletmenet (ügymenet)	3.1.4.1.	Üzletmenet folytonosságra	I	I			A szervezet rendelkezik érvényes üzletmenete-

folytonosság tervezése		vonatkozó eljárásrend										folytonosságra vonatkozó eljárásrenddel.
3.1.4. Üzletmenet (ügymenet) folytonosság tervezése	3.1.4.2.	Üzletmenet folytonossági terv informatikai erőforrás kiesésekre	I	I								A szervezet rendelkezik érvényes üzletmenete-folytonosságra tervvel erőforrás kiesésekre.
3.1.4. Üzletmenet (ügymenet) folytonosság tervezése	3.1.4.8.	Az elektronikus információs rendszer mentései	N	N								A szervezet nem rendelkezik rendszer mentési folyamattal.
3.1.4. Üzletmenet (ügymenet) folytonosság tervezése	3.1.4.9.	Az elektronikus információs rendszer helyreállítása és újraindítása	I	I								A szervezet rendelkezik dokumentált rendszerhelyreállítási renddel, melyet az informatikai szabályzatban fogalmaz meg.
3.1.6. EMBERI TÉNYEZŐKET FIGYELEMBE VEVŐ - SZEMÉLY - BIZTONSÁG	3.1.6.4.	Eljárás a jogviszony megszűnésekor	I	I								A szervezetnek van dokumentált jogosultság ellenőrzési eljárásrendje, mely magába foglalná a logikai hozzáférései jogok visszavonását, fizikai eszközök visszaszolgáltatását illetve a megfelelő szerepkörök feladatkörét.
3.1.6. EMBERI TÉNYEZŐKET FIGYELEMBE VEVŐ - SZEMÉLY - BIZTONSÁG	3.1.6.7.	Fegyelmi intézkedések	I	I								A szervezet rendelkezik dokumentált fegyelmi eljárásrenddel, melyet az informatikai szabályzatban fogalmaz meg.
3.1.6. EMBERI TÉNYEZŐKET FIGYELEMBE VEVŐ - SZEMÉLY - BIZTONSÁG	3.1.6.9.	Viselkedési szabályok az interneten	I	I								A szervezet rendelkezik érvényes interneten való kommunikáció szabályait leíró szabályokkal és vagy elvekkel vonatkozó eljárásrenddel.
3.1.7. TUDATOSSÁG ÉS KÉPZÉS	3.1.7.2.	Képzési eljárásrend	I	I								A szervezet tart ismétlődő információbiztonsági képzést, van érvényes dokumentált képzési eljárásrendje.
3.1.7. TUDATOSSÁG ÉS KÉPZÉS	3.1.7.3	Biztonság tudatosság képzés	I	I								A szervezet tart ismétlődő információbiztonsági képzést, van érvényes dokumentált képzési eljárásrendje.
3.2.1. FIZIKAI ÉS KÖRNYEZETI VÉDELEM	3.2.1.2.	Fizikai védelmi eljárásrend	I	I	I	I	I	I	I	I	I	A szervezetnek van érvényes fizikai védelmi eljárásrendje, mely az informatikai szabályzat részét képzi.
3.2.1. FIZIKAI ÉS KÖRNYEZETI VÉDELEM	3.2.1.3.	Fizikai belépési engedélyek	I	I	I	I	I	I	I	I	I	A szervezet vizsgálja illetve ellenőrzi a fizikai belépéseket.

3.2.1. FIZIKAI ÉS KÖRNYEZETI VÉDELEM	3.2.1.4.	A fizikai belépés ellenőrzése	I	I	I	I	I	I	I	I	I	I	A szervezet vizsgálja illetve ellenőrzi a fizikai belépési jogosultságokat.
3.3.1. LOGIKAI VÉDELMI INTÉZKEDÉSEK, ÁLTALÁNOS VÉDELMI INTÉZKEDÉSEK	3.3.1.1.	Engedélyezés	I	I	I	I	I	I	I	I	I	I	A szervezet dokumentáltan szabályozta az engedélyezési folyamtokat
3.3.1. LOGIKAI VÉDELMI INTÉZKEDÉSEK, ÁLTALÁNOS VÉDELMI INTÉZKEDÉSEK	3.3.1.4.	Személybiztonság	I										A szervezetben kiterjed a biztonsággal kapcsolatos eljárás vagy elvárás minden érintettre
3.3.2. LOGIKAI VÉDELMI INTÉZKEDÉSEK, TERVEZÉS	3.3.2.2.	Rendszerbiztonsági terv	I	I	I	I	I	I	I	I	I	I	A szervezet rendelkezik rendszerbiztonsági tervvel.
3.3.2. LOGIKAI VÉDELMI INTÉZKEDÉSEK, TERVEZÉS	3.3.2.3.	Cselekvési terv	I				I			I			A szervezet a megállapított hiányosságok kezelésére rendelkezik cselekvési tervvel.
3.3.2. LOGIKAI VÉDELMI INTÉZKEDÉSEK, TERVEZÉS	3.3.2.4.	Személyi biztonság	I		I		I		I		I		A szervezet rendelkezik az információs rendszer hozzáférését definiáló engedélyezési eljárással és engedélyek kiadásával.
3.3.3. LOGIKAI VÉDELMI INTÉZKEDÉSEK,BESZERZÉS	3.3.3.2.	A rendszer fejlesztési életciklusa	I			I			I				A szervezetben a fejlesztés során figyelembe veszik a teljes életciklust.
3.3.6. KONFIGURÁCIÓKEZELÉS	3.3.6.1.	Konfigurációkezelési eljárásrend	I					I					A szervezet rendelkezik konfiguráció kezelési eljárásrenddel melyet az Információ biztonsági szabályzatban fogalmazott meg.
3.3.6. KONFIGURÁCIÓKEZELÉS	3.3.6.2.	Alapkonfiguráció	N										A szervezet nem rendelkezik érvényes konfiguráció kezelési eljárásrenddel az egyes információbiztonsági rendszereire.
3.3.6. KONFIGURÁCIÓKEZELÉS	3.3.6.8.	Elektronikus információs rendszerelem leltár	N			N			N				A szervezet nem készít és vezet leltárt az infrastrukturális eleméről.
3.3.6. KONFIGURÁCIÓKEZELÉS	3.3.6.10.	A szoftverhasználat korlátozásai	I			I			I				A szervezet rendelkezik érvényes szoftverkezelési eljárásrenddel, melyet az informatikai szabályzatban fogalmaz meg.
3.3.6. KONFIGURÁCIÓKEZELÉS	3.3.6.11.	A felhasználó által telepített szoftverek	N			N			N				A szervezet nem érvényesíti a szoftverkezelési szabályokat.

3.3.7. KARBANTARTÁS	3.3.7.1.	Rendszer karbantartási eljárásrend	I			I			A szervezet az informatikai szabályzatában fogalmazza meg a rendszer karbantartási ejárásrendjét a rendszergazda feladatai között.
3.3.7. KARBANTARTÁS	3.3.7.2.	Rendszeres karbantartás	N	N	N	N	N	N	A szervezet az informatikai szabályzatában fogalmazza meg a rendszer karbantartási ejárásrendjét a rendszergazda feladatai között, ami a gyakorlatban nem valósul meg.
3.3.8. ADATHORDOZÓK VÉDELME	3.3.8.1.	Adathordozók védelmére vonatkozó eljárásrend	I			I			A szervezetnek van érvényes eljárásrendje az adat hordozók védelmére vonatkozóan.
3.3.8. ADATHORDOZÓK VÉDELME	3.3.8.2.	Hozzáférés az adathordozókhoz	N						A szervezet nem vezet nyilvántartást, hogy kik férhetnek hozzá az egyes adathordozókhoz.
3.3.8. ADATHORDOZÓK VÉDELME	3.3.8.6.	Adathordozók törlése	I			I			A szervezetnek van érvényes szabályozása a adathordozók törlésének technikájáról.
3.3.8. ADATHORDOZÓK VÉDELME	3.3.8.7.	Adathordozók használata	I						A szervezet az informatikai szabályzatában fogalmazza meg az egyes adathordozók használatát az alkalmazott információs rendszereken.
3.3.9. AZONOSÍTÁS ÉS HITELESÍTÉS	3.3.9.1.	Azonosítási és hitelesítési eljárásrend	I			I			A szervezet jelenleg rendelkezik dokumentált azonosítási és hitelesítési eljárásrenddel. Az érvényben lévő informatikai szabályzat rögzít a felhasználói jogosultságok nyilvántartását, folyamat a gyakorlatban követve.
3.3.9. AZONOSÍTÁS ÉS HITELESÍTÉS	3.3.9.2.	Azonosítás hiteleítés	I						A telepített illetve az online rendszerek használata mind felhasználó azonosításhoz kötött.
3.3.9. AZONOSÍTÁS ÉS HITELESÍTÉS	3.3.9.4.	Azonosító kezelés	I			I		I			Az azonosító kezelés jelenleg az online rendszerek esetében központilag szabályozott.
3.3.9. AZONOSÍTÁS ÉS HITELESÍTÉS	3.3.9.5.	A hitelesítésre szolgáló eszközök kezelése	I	I	I	I	I	I	I	I	I	I	A szervezet az IBSZ-ben fogalmazta meg a hitelesítésre használt eszközök kezelésére vonatkozó szabályrendszert. ASP-ben használatos.

3.3.9. AZONOSÍTÁS ÉS HITELESÍTÉS	3.3.9.6.	A hitelesítésre szolgáló eszköz visszacsatolása	I										ASP
3.3.9. AZONOSÍTÁS ÉS HITELESÍTÉS	3.3.9.8.	Azonosítás és hitelesítés (szervezeten kívüli felhasználók)	NA					NA					Az a kérdés a szervezet működéséhez nem releváns.
3.3.9. AZONOSÍTÁS ÉS HITELESÍTÉS	3.3.9.8.2.	Hitelesítésszolgáltatók tanúsítványának elfogadása	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	Az a kérdés a szervezet működéséhez nem releváns.
3.3.10. HOZZÁFÉRÉS ELLENŐRZÉSE	3.3.10.1.	Hozzáférés ellenőrzési eljárásrend	I					I					A szervezetnek jelenleg van érvényes dokumentált hozzáférés ellenőrzési eljárásrendje.
3.3.10. HOZZÁFÉRÉS ELLENŐRZÉSE	3.3.10.2.	Felhasználói fiókok kezelése	I	I	I	I	I	I	I	I	I	I	A szervezet a felhasználói fiókok kezelését az IBSZ-ben fogalmazta meg.
3.3.10. HOZZÁFÉRÉS ELLENŐRZÉSE	3.3.10.3.	Hozzáférés ellenőrzés érvényesítése	I										A szervezetnek van érvényes dokumentált hozzáférés ellenőrzési eljárásrendje.
3.3.10. HOZZÁFÉRÉS ELLENŐRZÉSE	3.3.10.12.	Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek	I					I					Nincs olyan tevékenység melyet azonosítás, hitelesítés nélkül végre lehet hajtani.
3.3.10. HOZZÁFÉRÉS ELLENŐRZÉSE	3.3.10.16.	Külső elektronikus információs rendszerek használata	I					I					A szervezet szabályozza a külső vagy távoli hozzáférés feltételeit az információs rendszerekhez. A kérdés az online rendszerekre nem alkalmazható, mivel azok minden internet hozzáféréssel rendelkező eszközről elérhetők.
3.3.10. HOZZÁFÉRÉS ELLENŐRZÉSE	3.3.10.18.	Nyilvánosan elérhető tartalom	I			I		I			I		A szervezet kijelöli azon személyek körét, akik jogosultak nyilvánosan hozzáférhető adtatok közzétételére.
3.3.11. RENDSZER- ÉS INFORMÁCIÓSÉRTETLENSÉG	3.3.11.2.	Rendszer- és információsértetlenségre vonatkozó eljárásrend	I					I					A szervezet rendelkezik rendszer- és információsértetlenségre vonatkozó eljárásrenddel az infrastrukturális rendszerekre vonatkozóan.
3.3.11. RENDSZER- ÉS INFORMÁCIÓSÉRTETLENSÉG	3.3.11.3.	Hibajavítás	I			I		I			I		A szervezet rendelkezik belső eljárásrenddel, mely az információs rendszerek hibajavítását szabályozza. Az alkalmazás szintű telepített rendszerek esetében a hibajavító csomagokat külső hordozható médián vagy online letölthető formába kapja meg, az infrastrukturális elemek esetén a frissítéseket online manuális vagy automatikus úton tölti le.

3.3.11. RENDSZER- ÉS INFORMÁCIÓSÉRTETLENSÉG	3.3.11.4.	Kártékony kódok elleni védelem	I		I		I		I		A szervezet információs rendszerei minden esetben kártékony kódok ellenei védelmi funkcióval vannak ellátva. A munkaállomásokra telepítésre kerültek a védelmi funkciót betöltő rendszer, és annak felügyelete illetve karbantartása megoldott.
3.3.11. RENDSZER- ÉS INFORMÁCIÓSÉRTETLENSÉG	3.3.11.5.	Az elektronikus információs rendszer felügyelete	I		I		I		I	I	A szervezet rendelkezik logikai behatolás védelmi illetve egyéb hálózat felügyeleti eszközzel.
3.3.11. RENDSZER- ÉS INFORMÁCIÓSÉRTETLENSÉG	3.3.11.12.	A kimeneti információ kezelése és megőrzése	I								Az érintett szervezet az elektronikus információs rendszer kimeneti információit a jogszabályokkal, szabályzatokkal és az üzemeltetési követelményekkel összhangban szabályozza.
3.3.12. NAPLÓZÁS ÉS ELSZÁMOLTATHATÓSÁG	3.3.12.1.	Naplózási eljárásrend	I				I				A szervezetnek van alkalmazott naplózási eljárásrendje. Naplózási adatok lokálisan az infrastrukturális eszközökön tárolódnak, de azoknak tartalmát, azokhoz való hozzáférést a nem felügyelik.
3.3.12. NAPLÓZÁS ÉS ELSZÁMOLTATHATÓSÁG	3.3.12.2.	Naplózható események	N		N		N				A szervezetnek van alkalmazott naplózási eljárásrendje. Naplózási adatok lokálisan az infrastrukturális eszközökön tárolódnak, de azoknak tartalmát, azokhoz való hozzáférést a nem felügyelik.
3.3.12. NAPLÓZÁS ÉS ELSZÁMOLTATHATÓSÁG	3.3.12.3.	Naplóbejegyzések tartalma	N								A szervezetnek van alkalmazott naplózási eljárásrendje. Naplózási adatok lokálisan az infrastrukturális eszközökön tárolódnak, de azoknak tartalmát, azokhoz való hozzáférést a nem felügyelik.
3.3.12. NAPLÓZÁS ÉS ELSZÁMOLTATHATÓSÁG	3.3.12.8.	Időbélyegek	N								A szervezetnek van alkalmazott naplózási eljárásrendje. Naplózási adatok lokálisan az infrastrukturális eszközökön tárolódnak, de azoknak tartalmát, azokhoz való hozzáférést a nem felügyelik.

3.3.12. NAPLÓZÁS ÉS ELSZÁMOLTATHATÓSÁG	3.3.12.9.	A naplóinformációk védelme	N			A szervezetnek van alkalmazott naplózási eljárásrendje. Naplózási adatok lokálisan az infrastrukturális eszközökön tárolódnak, de azoknak tartalmát, azokhoz való hozzáférést a nem felügyelik.
3.3.12. NAPLÓZÁS ÉS ELSZÁMOLTATHATÓSÁG	3.3.12.11.	A naplóbejegyzések megőrzése	N			A szervezetnek van alkalmazott naplózási eljárásrendje. Naplózási adatok lokálisan az infrastrukturális eszközökön tárolódnak, de azoknak tartalmát, azokhoz való hozzáférést a nem felügyelik.
3.3.12. NAPLÓZÁS ÉS ELSZÁMOLTATHATÓSÁG	3.3.12.12.	Naplógenerálás	N	N	N	A szervezetnek van alkalmazott naplózási eljárásrendje. Naplózási adatok lokálisan az infrastrukturális eszközökön tárolódnak, de azoknak tartalmát, azokhoz való hozzáférést a nem felügyelik.
3.3.13. RENDSZER- ÉS KOMMUNIKÁCIÓVÉDELEM	3.3.13.1.	Rendszer- és kommunikációvédelmi eljárásrend	I	I		A szervezetnek van alkalmazott idevonatkozó eljárásrendje.
3.3.13. RENDSZER- ÉS KOMMUNIKÁCIÓVÉDELEM	3.3.13.6.	A határok védelme	I	I	I	A szervezet rendelkezik külső határvédelmi funkcióval, a kulcsfontosságú belő határain történő kommunikációt nem ellenőrzi.
3.3.13. RENDSZER- ÉS KOMMUNIKÁCIÓVÉDELEM	3.3.13.10.	Kriptográfiai kulcs előállítása és kezelése	NA			A szervezet számára ez a kontroll nem érvényes.
3.3.13. RENDSZER- ÉS KOMMUNIKÁCIÓVÉDELEM	3.3.13.11.	Kriptográfiai védelem	NA			A szervezet számára ez a kontroll nem érvényes.
3.3.13. RENDSZER- ÉS KOMMUNIKÁCIÓVÉDELEM	3.3.13.12.	Együttműködésen alapuló számítástechnikai eszközök	NA			A szervezet nem engedélyezi az együttműködésen alapuló eszközök távoli hozzáférését illetve kezelését.
3.3.13. RENDSZER- ÉS KOMMUNIKÁCIÓVÉDELEM	3.3.13.22.	A folyamatok elkülönítése	I			A szervezet számára ez a kontroll megfelelően teljesül

ASP MEGFELELÉS A „2018.06.18-I (VER.2) TÁJÉKOZTATÁS AZ ÖNKORMÁNYZATI ASP RENDSZEREKHEZ CSATLAKOZÁSHOZ MEGVALÓSÍTANDÓ INFORMATIKAI BIZTONSÁGI KÖVETELMÉNYEKRŐL” ÉRTÉKELÉSE.

Alpont	NEIH sorszám	Intézkedés típusa	Értékelés					Megjegyzés
3.1.3. Rendszer és szolgáltatásbeszerzés	3.1.3.1.	Beszerzési eljárásrend	I				I	
3.1.3. Rendszer és szolgáltatásbeszerzés	3.1.3.2	Erőforrás igény felmérés	I				I	
3.1.4. ÜZLETMENET- (ÜGYMENET-) FOLYTONOSSÁG TERVEZÉSE	3.1.3.3.	Beszerzések	I	I	I	I	I	
3.1.4. ÜZLETMENET- (ÜGYMENET-) FOLYTONOSSÁG TERVEZÉSE	3.1.3.3.2.	A védelem szempontjainak érvényesítése a beszerzés során	I				I	
3.1.4. ÜZLETMENET- (ÜGYMENET-) FOLYTONOSSÁG TERVEZÉSE	3.1.4.2.4.	Kritikus rendszerelemek meghatározása	I					
3.1.4. ÜZLETMENET- (ÜGYMENET-) FOLYTONOSSÁG TERVEZÉSE	3.1.4.3.	A folyamatos működésre felkészítő képzés	I				I	
3.1.4. ÜZLETMENET- (ÜGYMENET-) FOLYTONOSSÁG TERVEZÉSE	3.1.4.5.3.	Üzletmenet-folytonosság elérhetőség	I					
3.1.4. ÜZLETMENET- (ÜGYMENET-) FOLYTONOSSÁG TERVEZÉSE	3.1.4.7.	Infokommunikációs szolgáltatások	I					

3.1.4. ÜZLETMENET- (ÜGYMENET-) FOLYTONOSSÁG TERVEZÉSE	3.1.4.7.2.	Szolgáltatások prioritása	I						
3.1.6. EMBERI TÉNYEZŐKET FIGYELEMBE VEVŐ - SZEMÉLY - BIZTONSÁG	3.1.6.1	Személybiztonsági eljárásrend	I						
3.1.6. EMBERI TÉNYEZŐKET FIGYELEMBE VEVŐ - SZEMÉLY - BIZTONSÁG	3.1.6.2.	Munkakörök, feladatok biztonsági szempontú besorolása	I		I		I		
3.1.6. EMBERI TÉNYEZŐKET FIGYELEMBE VEVŐ - SZEMÉLY - BIZTONSÁG	3.1.6.3.	A személyek ellenőrzése	I		I		I		
3.1.6. EMBERI TÉNYEZŐKET FIGYELEMBE VEVŐ - SZEMÉLY - BIZTONSÁG	3.1.6.5.	Az áthelyezések, átirányítások és kirendelések kezelése	I		I		I		I
3.1.6. EMBERI TÉNYEZŐKET FIGYELEMBE VEVŐ - SZEMÉLY - BIZTONSÁG	3.1.6.6.	Az érintett szervezettel szerződéses jogviszonyban álló (külső) szervezetre vonatkozó követelmények	I	I	I	I	I		
3.1.6. EMBERI TÉNYEZŐKET FIGYELEMBE VEVŐ - SZEMÉLY - BIZTONSÁG	3.1.6.8.	Belső egyeztetés	I						
3.1.7. TUDATOSSÁG ÉS KÉPZÉS	3.1.7.1.	Kapcsolattartás az elektronikus információbiztonság jogszabályban meghatározott szervezetrendszerével és az e célt szolgáló ágazati szervezetekkel	I		I		I		
3.1.7. TUDATOSSÁG ÉS KÉPZÉS	3.1.7.4.	Belső fenyegetés	I						
3.1.7. TUDATOSSÁG ÉS KÉPZÉS	3.1.7.5.	Szerepkör, vagy feladat alapú biztonsági képzés	I		I		I		

3.1.7. TUDATOSSÁG ÉS KÉPZÉS	3.1.7.6	A biztonsági képzésre vonatkozó dokumentációk	I		I		
3.2.1. FIZIKAI ÉS KÖRNYEZETI VÉDELEM	3.2.1.5.	Hozzáférés az adatátviteli eszközökhöz és csatornákhoz	I				
3.2.1. FIZIKAI ÉS KÖRNYEZETI VÉDELEM	3.2.1.6.	A kimeneti eszközök hozzáférés ellenőrzése	I				
3.2.1. FIZIKAI ÉS KÖRNYEZETI VÉDELEM	3.2.1.7.	A fizikai hozzáférések felügyelete	I	I	I	I	
3.2.1. FIZIKAI ÉS KÖRNYEZETI VÉDELEM	3.2.1.7.2.	Behatolás riasztás, felügyeleti berendezések	I				
3.2.1. FIZIKAI ÉS KÖRNYEZETI VÉDELEM	3.2.1.8.	A látogatók ellenőrzése	I		I		
3.2.1. FIZIKAI ÉS KÖRNYEZETI VÉDELEM	3.2.1.9.	Áramellátó berendezések és kábelezés	I				
3.2.1. FIZIKAI ÉS KÖRNYEZETI VÉDELEM	3.2.1.12.	Tűzvédelem	I				
3.2.1. FIZIKAI ÉS KÖRNYEZETI VÉDELEM	3.2.1.14.	Víz-, és más, csővezetéken szállított anyag okozta kár elleni védelem	I				
3.2.1. FIZIKAI ÉS KÖRNYEZETI VÉDELEM	3.2.1.15.	Be- és kiszállítás	I				
3.2.1. FIZIKAI ÉS KÖRNYEZETI VÉDELEM	3.2.1.16.	Az elektronikus információs rendszer elemeinek elhelyezése	I				
3.2.1. FIZIKAI ÉS KÖRNYEZETI VÉDELEM	3.2.1.19.	Karbantartók	I	I	I		
3.2.1. FIZIKAI ÉS KÖRNYEZETI VÉDELEM	3.2.1.19.3.	Időben történő javítás	I				

3.3.1. ÁLTALÁNOS VÉDELMI INTÉZKEDÉSEK	3.3.1.3.	Az elektronikus információs rendszer kapcsolódásai	I			I			
3.3.1. ÁLTALÁNOS VÉDELMI INTÉZKEDÉSEK	3.3.1.3.2.	Belső rendszerkapcsolatok	I						
3.3.1. ÁLTALÁNOS VÉDELMI INTÉZKEDÉSEK	3.3.1.3.3.	Külső kapcsolódásokra vonatkozó korlátozások	I						
3.3.6. KONFIGURÁCIÓKEZELÉS	3.3.6.7.	Legszűkebb funkcionalitás	I			I			
3.3.6. KONFIGURÁCIÓKEZELÉS	3.3.6.8.4.	Duplikálás elleni védelem	I						
3.3.7. KARBANTARTÁS	3.3.7.3.2.	Adathordozó ellenőrzés	I						
3.3.7. KARBANTARTÁS	3.3.7.4.	Távoli karbantartás	I	I	I	I	I		
3.3.8. ADATHORDOZÓK VÉDELME	3.3.8.4.	Adathordozók tárolása	I			I			
3.3.8. ADATHORDOZÓK VÉDELME	3.3.8.5.	Adathordozók szállítása	I	I		I		I	
3.3.8. ADATHORDOZÓK VÉDELME	3.3.8.5.2.	Kriptográfiai védelem	I						
3.3.8. ADATHORDOZÓK VÉDELME	3.3.8.7.2.	Ismeretlen tulajdonos	I						
3.3.9. AZONOSÍTÁS ÉS HITELESÍTÉS	3.3.9.5.2.	Jelszó (tudás) alapú hitelesítés	I	I		I		I	
3.3.9. AZONOSÍTÁS ÉS HITELESÍTÉS	3.3.9.5.3.	Birtoklás alapú hitelesítés	I						

3.3.9. AZONOSÍTÁS ÉS HITELESÍTÉS	3.3.9.5.5.	Személyes vagy megbízható harmadik fél általi regisztráció	I			
3.3.10. HOZZÁFÉRÉS ELLENŐRZÉSE	3.3.10.5.	A felelősségek szétválasztása	I	I	I	
3.3.10. HOZZÁFÉRÉS ELLENŐRZÉSE	3.3.10.6.	Legkisebb jogosultság elve	I			
3.3.10. HOZZÁFÉRÉS ELLENŐRZÉSE	3.3.10.6.2.	Jogosult hozzáférés a biztonsági funkciókhoz	I			
3.3.10. HOZZÁFÉRÉS ELLENŐRZÉSE	3.3.10.6.3.	Nem privilegizált hozzáférés a biztonsági funkciókhoz	I			
3.3.10. HOZZÁFÉRÉS ELLENŐRZÉSE	3.3.10.6.4.	Privilegizált fiókok	I			
3.3.10. HOZZÁFÉRÉS ELLENŐRZÉSE	3.3.10.10.	A munkaszakasz zárolása	I	I		
3.3.10. HOZZÁFÉRÉS ELLENŐRZÉSE	3.3.10.10.2.	Képernyőtakarás	I			
3.3.10. HOZZÁFÉRÉS ELLENŐRZÉSE	3.3.10.11.	A munkaszakasz lezárása	I			
3.3.10. HOZZÁFÉRÉS ELLENŐRZÉSE	3.3.10.14.	Vezeték nélküli hozzáférés	I	I		
3.3.10. HOZZÁFÉRÉS ELLENŐRZÉSE	3.3.10.15.	Mobil eszközök hozzáférés ellenőrzése	I	I		
3.3.10. HOZZÁFÉRÉS ELLENŐRZÉSE	3.3.10.15.2.	Titkosítás	I	I		
3.3.10. HOZZÁFÉRÉS ELLENŐRZÉSE	3.3.10.16.2.	Korlátozott használat	I	I		

3.3.10. HOZZÁFÉRÉS ELLENŐRZÉSE	3.3.10.16.3.	Hordozható adattároló eszközök	I							
3.3.11. RENDSZER- ÉS INFORMÁCIÓSÉRTETLENSÉG	3.3.11.4.3.	Automatikus frissítés	I							
3.3.11. RENDSZER- ÉS INFORMÁCIÓSÉRTETLENSÉG	3.3.11.6.	Biztonsági riasztások és tájékoztatások	I	I	I	I	I	I		
3.3.11. RENDSZER- ÉS INFORMÁCIÓSÉRTETLENSÉG	3.3.11.10.	Bemeneti információ ellenőrzés	I							

V.2. Cselekvési terv az elvárt védelmi intézkedések megvalósítására

I. Biztonsági szint 3.1. ADMINISZTRATÍV VÉDELMI INTÉZKEDÉSEK	II. Biztonsági szint 3.2. FIZIKAI VÉDELMI INTÉZKEDÉSEK 3.3. LOGIKAI VÉDELMI INTÉZKEDÉSEK	Határidő	Feladatok	Felelős személy	Megjegyzés
3.1.2.1. Kockázatelemzési eljárásrend		2021.04.18.	Az érintett szervezet megfogalmazza, és az érintett szervezetre érvényes követelmények szerint dokumentálja, valamint az érintett szervezeten belül kihirdeti a kockázatelemzési és kockázatkezelési eljárásrendet, mely a kockázatelemzési és kockázatkezelési szabályzat és az ehhez kapcsolódó ellenőrzések megvalósítását segíti elő;	IBF	
3.1.4.8. Az elektronikus információs rendszer mentései		2021.04.18.	Az érintett szervezet meghatározott gyakorisággal mentést végez az elektronikus információs rendszerben tárolt felhasználószintű információkról, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal	Informatikus	
	3.3.6.2. Alapkonfiguráció	2021.04.18.	Az érintett szervezet az elektronikus információs rendszereihez egy-egy alapkonfigurációt fejleszt ki, dokumentálja és karbantartja ezt, valamint leltárba foglalja a rendszer lényeges elemeit.	Informatikus	
	3.3.6.8. Elektronikus információs rendszerelem leltár	2021.04.18.	Az érintett szervezet: leltárt készít az elektronikus információs rendszer elemeiről; meghatározott gyakorisággal felülvizsgálja és frissíti az elektronikus információs rendszerelem leltárt;	Informatikus	
	3.3.6.11. A felhasználó által telepített szoftverek	2021.04.18.	Az érintett szervezet: megfogalmazza, a szervezetre érvényes követelmények szerint dokumentálja, és a szervezeten belül kihirdeti azokat a szabályokat, amelyek meghatározzák a szoftverek felhasználó általi telepítési lehetőségét; érvényesíti a szoftvertelepítésre vonatkozó szabályokat az érintett szervezet által meghatározott módszerek szerint; meghatározott gyakorisággal ellenőrzi a szabályok betartását.	Informatikus	
	3.3.7.2. Rendszeres karbantartás	2021.04.18.	Az érintett szervezet: a karbantartásokat és javításokat ütemezetten hajtja végre, dokumentálja és felülvizsgálja a karbantartásokról és javításokról készült feljegyzéseket a gyártó vagy a forgalmazó specifikációinak és a szervezeti követelményeknek megfelelően; jóváhagyja és ellenőrzi az összes karbantartási tevékenységet, függetlenül attól, hogy azt a helyszínen vagy távolról végzik, és függetlenül attól, hogy a berendezést a helyszínen, vagy másutt tartják karban; az ezért felelős személyek jóváhagyásához köti az elektronikus információs rendszer vagy a rendszerelemek kiszállítását a szervezeti létesítményből; az elszállítás előtt minden adatot és információt - mentést követően - töröl a berendezésről; ellenőrzi, hogy a berendezések a karbantartási vagy javítási tevékenységek után is megfelelően működnek-e, és biztonsági ellenőrzésnek veti alá azokat; csatolja a meghatározott, karbantartással kapcsolatos információkat a karbantartási nyilvántartáshoz.	Informatikus	
	3.3.8.2. Hozzáférés az adathordozókhoz	2021.04.18.	Az érintett szervezet az egyes adathordozó típusokhoz való hozzáférésre feljogosított személyek körét, jogosítványuk tartalmát meghatározza.	Informatikus	
	3.3.12.2. Naplózható események	2021.04.18.	meghatározza a naplózható és naplózandó eseményeket, és felkészíti erre az elektronikus információs rendszerét; egyezteti a biztonsági napló funkciókat a többi, naplóval kapcsolatos információt igénylő szervezeti egységgel, hogy növelje a kölcsönös támogatást, és hogy iránymutatással segítse a naplózható események kiválasztását;	Informatikus	

			megvizsgálja, hogy a naplózható események megfelelőnek tekinthetők-e a biztonsági eseményeket követő tényfeltáró vizsgálatok támogatásához.		
	3.3.12.3. Naplóbejegyzések tartalma	2021.04.18.	Az elektronikus információs rendszer a naplóbejegyzésekben gyűjtsön be elegendő információt ahhoz, hogy ki lehessen mutatni, hogy milyen események történtek, miből származtak ezek az események, és mi volt ezen események kimenetele.	Informatikus	
	3.3.12.8. Időbélyegek	2021.04.18.	Az elektronikus információs rendszer: belső rendszerórákat használ a naplóbejegyzések időbélyegeinek előállításához; időbélyegeket rögzít a naplóbejegyzésekben a koordinált világidőhöz - úgynevezett UTC - vagy a Greenwichi középidőhöz - úgynevezett GMT - rendelhető módon, megfelelve az érintett szervezet által meghatározott időmérési pontosságnak.	Informatikus	
	3.3.12.9. A naplóinformációk védelme	2021.04.18.	Az elektronikus információs rendszer megvédi a naplóinformációt és a napló kezelő eszközöket a jogosulatlan hozzáféréssel, módosítással és törléssel szemben.	Informatikus	
	3.3.12.11. A naplóbejegyzések megőrzése	2021.04.18.	Az érintett szervezet a naplóbejegyzéseket meghatározott - a jogszabályi és az érintett szervezeten belüli információ megőrzési követelményeknek megfelelő - időtartamig megőrzi a biztonsági események utólagos kivizsgálásának biztosítása érdekében.	Informatikus	
	3.3.12.12. Naplógenerálás	2021.04.18.	Az elektronikus információs rendszer: biztosítja a naplóbejegyzés generálási lehetőségét a 3.3.12.2. pontban meghatározott, naplózható eseményekre; lehetővé teszi meghatározott személyeknek vagy szerepköröknek, hogy kiválasszák, hogy mely naplózható események legyenek naplózva az elektronikus információs rendszer egyes elemeire; naplóbejegyzéseket állít elő a 3.3.12.2. pont szerinti eseményekre a 3.3.12.3. pontban meghatározott tartalommal.	Informatikus	